CLAIMS

Sub B1

1. An apparatus for selectively encrypting data sent over a network between a server and a client, comprising:

means for parsing a first portion of the data from a second portion of the data;

means for encrypting only the first portion of the data; and

means for combining the encrypted first portion of the data with the second portion of the data which is not encrypted.

2. An apparatus of claim 1, wherein the data is streaming data.

3. An apparatus of claim 1, wherein the first portion of the data is information constituting payload data and comprising multimedia data.

4. An apparatus of claim 1, wherein the second portion of the data is non-payload data containing at least one of a header, control data and routing data.

5. An apparatus of claim 1, further comprising means for sending the combined first and second portions of the data over the network to the client.

6. An apparatus of claim 1, further comprising means for receiving the data from the server.

7. An apparatus of claim 1, further comprising means for establishing a data stream between the server and the client.

B1 cont

8. An apparatus of claim 1, further comprising key-negotiating means for negotiating an encryption key with the client.

9. An apparatus of claim 8, wherein key negotiation can occur dynamically throughout the process of streaming and encryption.

10. An apparatus of claim 9, wherein encryption by the encrypting means is transparent to the server.

11. An apparatus of claim 8, wherein key negotiation can determine the correctness of the result.

12. An apparatus of claim 1, further comprising decrypting means installed at the client for decrypting the combined first and second portions of the data.

13. An apparatus of claim 1, wherein the parsing means parses the data into different portions based on media format.

14. An apparatus of claim 1, wherein the encrypting means encrypts the first portion of the data based on media format.

15. An apparatus of claim 1, wherein the apparatus is implemented as one of an application and plug-in object.

16. A server equipped with the apparatus of claim 1.

17. A method for selectively encrypting data composed of first and second portions which differ from each other in at least on characteristic, the data being sent over a network between a server and a client, comprising:

B1 Con't

parsing the data into the first and second portions;

encrypting only the first portion of the data; and

sending the encrypted first portion and the second portion of the data over the network to the client.

18. A method of claim 17, further comprising receiving the data from the server.

19. A method of claim 17, further comprising determining whether a stream is established between the server and the client.

20. A method of claim 17, further comprising negotiating an encryption key with the client.

21. A method of claim 20, wherein the data is streaming data sent from the server during a streaming session and said step of negotiating the encryption key is carried out throughout the streaming session.

~~22. A method of claim 20, further comprising terminating a streaming session if it is found that the encryption key is invalid.~~

~~23. A method claim 17, wherein the encryption key is negotiated with a decryption shim on the client.~~

B1 cont

~~24. A method of claim 17, further comprising determining whether the data is streaming data.~~

~~25. A method of claim 24, further comprising ignoring the data if the data is not streaming data.~~

~~26. A method of claim 17, further comprising determining whether a shim is present on the client.~~

~~27. A method claim 26, further comprising deploying a shim if it is determined that the shim is not present on the client.~~

~~28. A method of claim 17, further comprising determining whether an encryption key is current.~~

~~29. A method of claim 17, wherein the data includes a payload data portion and at least one of a header, control data and routing data.~~

30. A method of claim 29, wherein the first portion of the data is the payload data portion.

B1 Cont

31. A method of claim 17, further comprising determining whether a packet is the last in a data stream.

32. A method of claim 31, further comprising receiving feedback from a decryption shim on the client if it is determined that the packet is not the last packet in the data stream.

33. A method of claim 17, further comprising determining whether the client is compromised.

34. A method of claim 33, further comprising continuing parsing the data into the first and second portions if it is determined that the client is not compromised.

35. A method of claim 33, further comprising terminating a streaming session if it is determined that the client is compromised.

36. A method for decrypting, at a client, data composed of the first and second portions which differ from each other in at least on characteristic, the data being sent over a network to the client from an encryption source which encrypts the first portion, comprising:

~~receiving the data sent over the network from the encryption source to the client;~~

~~parsing the data into the first and second portions;~~

~~decrypting only the first portion of the data; and~~

~~passing the decrypted first portion of the data to a higher level of operations.~~

B1 cont

~~37. A method of claim 36, further comprising determining whether the data is an encrypted stream.~~

~~38. A method of claim 37, further comprising passing the data to higher layers when it is determined that the data is an encrypted stream.~~

~~39. A method of claim 36, further comprising negotiating a decryption key with the encryption source.~~

~~40. A method of claim 39, wherein the data is streaming data sent from the encryption source during a streaming session and said step of negotiating the decryption key is carried out throughout the streaming session.~~

~~41. A method of claim 39, further comprising termination of the encrypted stream if the encryption key is invalid.~~

~~42. A method of claim 36, wherein the first portion of the data is a payload data portion.~~

~~43. A method of claim 36, further comprising determining whether a packet is a last packet in a data stream.~~

B1 cont

~~44. A method of claim 43, further comprising sending feedback to the encryption source if it is determined that the packet is not the last packet in the data stream.~~

~~45. A method of claim 36, further comprising determining whether the client is compromised.~~

~~46. A method of claim 45, further comprising continuing parsing the data into the first and second portions if it is determined that the client is not compromised.~~

~~47. A method of claim 45, further comprising terminating a streaming session if it is determined that a packet is a last packet in a data stream or if the client is compromised.~~

add B2